

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2010-11

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2010-ACT-011>

Gestion du document

Référence	CERTA-2010-ACT-011
Titre	Bulletin d'actualité 2010-11
Date de la première version	19 mars 2010
Date de la dernière version	–
Source(s)	–
Pièce(s) jointe(s)	Aucune

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

Le bulletin d'actualité est disponible dans son intégralité et au format PDF à l'adresse suivante :

<http://www.certa.ssi.gouv.fr/site/CERTA-2010-ACT-011.pdf>

Un extrait du bulletin, ne reprenant que les articles de la semaine, se trouve en HTML à l'adresse suivante :

<http://www.certa.ssi.gouv.fr/site/CERTA-2010-ACT-011/>

1 Incident de la semaine

Campagne de fausses cartes de vœux virtuelles

Un de nos correspondants nous a informés que son serveur de messagerie était inondé de messages invitant les destinataires à consulter une carte de vœux virtuelle en ligne. Bien évidemment, cette prétendue « carte » est en fait un code malveillant. Cet incident n'a rien d'exceptionnel, néanmoins son analyse soulève deux points intéressants :

- la liste des destinataires était relativement précise et ne contenait que peu d'erreurs. Ces listes sont parfois constituées à partir d'informations collectées sur les serveurs Web. L'expérience montre que de larges fichiers, voire des bases de données, contenant des adresses de messagerie sont parfois déposés sur des sites Web et laissés accessibles depuis l'Internet, soit par négligence, soit par insouciance ;
- l'envoi massif des courriers électroniques a reposé sur des scripts PHP déposés sur des sites compromis. Le CERTA rencontre souvent ce genre de fichiers lors de l'analyse d'intrusions sur des serveurs, en particulier lorsque ces derniers ont été utilisés à des fins de hameçonnage. Il n'est d'ailleurs pas rare qu'après « nettoyage » des pages de *phishing*, ces fameux scripts d'émission de messages électroniques (souvent appelés

phpmailer) soient « oubliés » par les administrateurs/webmestres. La meilleure pratique reste encore la réinstallation complète des serveurs compromis.

2 Durcissement de la configuration des systèmes Windows : désactivation des empreintes de type LM (4/8)

Windows met en œuvre deux algorithmes pour calculer les empreintes des mots de passe des comptes utilisateur :

- l’empreinte *LM* (ou « *hash LM* »), basée sur l’algorithme *DES* et utilisant un alphabet réduit. Il s’agit du mécanisme historique largement vulnérable ;
- l’empreinte *NTLM* (ou « *hash NTLM* »), basée sur l’algorithme *MD4* et utilisant le codage *Unicode*.

Il est recommandé de ne pas calculer les empreintes de type *LM* dans les bases *SAM* des comptes locaux ou dans les annuaires *Active Directory*, afin de réduire les possibilités de cryptanalyse des mots de passe. Seule la version *NTLM* doit être conservée. Cette recommandation s’applique tant pour les postes de travail que pour les serveurs.

Afin de ne pas calculer l’empreinte *LM* au prochain changement du mot de passe, il faut :

- sous Windows 2000, ajouter une clé de registre appelée *NoLMHash* sous la clé `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\` ;
- à partir de Windows XP, ajouter une valeur dénommée *NoLMHash* de type *DWORD* dont la donnée vaut 1 dans la clé `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\`.

Depuis Windows XP, la suppression de la génération des empreintes de type *LM* peut être configurée au travers des *Options de sécurité*. Le paramètre se situe dans l’arborescence *Paramètres de sécurité, Stratégies locales, Options de sécurité* et s’intitule « *Sécurité réseau : ne pas stocker de valeurs de hachage de niveau Lan Manager sur la prochaine modification du mot de passe* ».

L’invalidation de l’empreinte *LM* de la base des comptes n’est effective qu’au prochain changement de mot de passe de chaque utilisateur.

Cette recommandation doit être appliquée sur chaque station de travail afin que l’empreinte *LM* ne figure pas dans les bases de comptes locaux. En ce qui concerne les comptes du domaine, la configuration de la stratégie locale de sécurité doit être appliquée au niveau des contrôleurs de domaine.

De Windows 2000 à Windows 2003, les deux empreintes sont engendrées par défaut. En revanche, à partir de Windows Vista, le paramètre de non-génération est activé dans la configuration d’origine et seule l’empreinte *NTLM* est calculée.

Les détails de cette démarche sont décrits dans l’article de la base de connaissances Microsoft KB 299656 « Comment faire pour empêcher Windows de stocker un hachage LAN Manager de votre mot de passe dans Active Directory et dans les bases de données SAM locales ».

Documentation :

- Microsoft KB 299656 « Comment faire pour empêcher Windows de stocker un hachage LAN Manager de votre mot de passe dans Active Directory et dans les bases de données SAM locales » : <http://support.microsoft.com/kb/299656>

3 Code malveillant et tunnel DNS

La technique de *tunneling*, bien que relativement ancienne (CF. note du 29 août 2001 du CERTA), continue d’être régulièrement déclinée et utilisée. Cette semaine des chercheurs ont publié des logiciels établissant des connexions bidirectionnelles, entre un *shell* et l’extérieur, et cela en utilisant le protocole *DNS*.

3.1 Comment cela fonctionne

Pour réussir à mettre en place un tel tunnel *DNS*, l’attaquant doit disposer d’un serveur de noms en charge d’un domaine qu’il maîtrise tel que `mondomaine.tld`. Ainsi, toutes les requêtes à destination de `XXXXXXXXX.mondomaine.tld` seront traitées par ce dernier, et il suffit d’utiliser la partie `XXXXXXXX` pour faire sortir des informations. Pour envoyer des données dans l’autre sens, le serveur de noms impliqué peut utiliser le champ *TXT resource record field*, associé à l’adresse *IP* dans une réponse normale. Cette technique, qui permet de contourner un grand nombre de filtres, laisse des traces significatives dans les journaux des *DNS*

locaux. Entre autre, de nombreuses requêtes vers le même domaine de base et avec des sous domaines illisibles et sans signification. Attention, les données présentes dans ces journaux peuvent avoir des caractères personnels, et leur utilisation demande une certaine prudence.

3.2 Documentation

- Note d’information du CERTA du 29 août 2001, mise à jour le 7 octobre 2005, CERTA-2001-INF-003-001 : <http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-003/CERTA-2001-INF003.html>

4 Liens utiles

- Mémento sur les virus : <http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002/>
- Note d’information du CERTA sur l’acquisition de correctifs : <http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/>
- Note d’information du CERTA sur les systèmes obsolètes : <http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/>
- Note d’information du CERTA sur les bonnes pratiques concernant l’hébergement mutualisé : <http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/>
- Note d’information du CERTA sur les mots de passe : <http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/>
- Note d’information sur la terminologie d’usage au CERTA : <http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/>
- Note d’information du CERTA sur les enjeux de sécurité liés à une migration vers IPv6 : <http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004/>
- Unix security checklist version 2.0 du 8 octobre 2001 (Publication du CERT australien) : <http://www.auscert.org.au/render.html?it=1937>
- Note d’information du CERTA sur les risques associés aux clés USB : <http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-006/>
- Note d’information du CERTA sur les outils d’indexation et de recherche : <http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-009/>
- Note d’information du CERTA sur la gestion des noms de domaine : <http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-001/>
- Note d’information du CERTA sur le bon usage de PHP : <http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002/>

5 Rappel des avis émis

Dans la période du 12 au 18 mars 2010, le CERTA a émis les avis suivants :

- CERTA-2010-AVI-119 : Vulnérabilité dans dpkg
- CERTA-2010-AVI-120 : Vulnérabilités dans Apple Safari
- CERTA-2010-AVI-121 : Vulnérabilité dans les produits HP Small Form Factor et HP Microtower PC
- CERTA-2010-AVI-122 : Vulnérabilité du serveur HTTP d’IBM
- CERTA-2010-AVI-123 : Vulnérabilité dans sendmail pour IBM AIX
- CERTA-2010-AVI-124 : Multiples vulnérabilités dans OSSIM
- CERTA-2010-AVI-125 : Vulnérabilité dans Skype
- CERTA-2010-AVI-126 : Multiples vulnérabilités dans Google Chrome
- CERTA-2010-AVI-127 : Vulnérabilité dans le module mm_forum de TYPO3

Durant la même période, les avis suivants ont été mis à jour :

- CERTA-2010-AVI-081-001 : Multiples vulnérabilités dans Adobe Reader et Adobe Acrobat (mention de la branche 8x et mise à jour de la description.)

6 Actions suggérées

6.1 Respecter la politique de sécurité

La Politique de Sécurité des Systèmes d'Information (PSSI) est l'ensemble formalisé dans un document applicable, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection des systèmes d'information de l'organisme. Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'organisme à la sécurité de ses systèmes d'information. D'une manière générale, elle contient une partie relative aux éléments stratégiques de l'organisme (périmètre, contexte, enjeux, orientations stratégiques en matière de SSI, référentiel réglementaire, échelle de sensibilité, besoins de sécurité, menaces) et une partie relative aux règles de sécurité applicables. Elle constitue donc une traduction concrète de la stratégie de sécurité de l'organisme.

Quoique puisse suggérer ce document, la politique de sécurité en vigueur dans votre service doit primer.

Cette section précise néanmoins quelques mesures générales de nature à vous prémunir contre les agressions décrites dans ce document. En effet, la sécurité des systèmes d'information ne repose pas exclusivement sur des outils, mais aussi sur une organisation et des politiques.

6.2 Concevoir une architecture robuste

A la lumière des enseignements tirés de ce qui a été présenté dans les bulletins d'actualité, il convient de vérifier que les applications mises en oeuvre (ou à l'étude) ont une architecture qui résiste aux incidents décrits.

6.3 Appliquer les correctifs de sécurité

Le tableau 2 rappelle les avis du CERTA correspondant aux applications ou codes malveillants relatifs aux ports étudiés dans les sections précédentes.

6.4 Utiliser un pare-feu

L'application des correctifs sur un parc informatique important n'est probablement pas immédiate. Un pare-feu correctement configuré peut retenir certaines attaques informatiques le temps d'appliquer les correctifs. Cependant un pare-feu peut donner une illusion de protection. Cette protection est brisée par la moindre introduction d'un ordinateur nomade dans la partie protégée. On remarque qu'il y a de nombreux paquets rejetés à destination de ports légitimement utilisés par des applications de prise de main à distance. La téléadministration correspond à une demande qui grandit avec la taille du parc à gérer. Les paquets rejetés montrent le risque associé à ce type d'application. Ce risque peut être amoindri par l'usage correct d'un pare-feu.

6.5 Analyser le réseau

De nombreux paquets rejetés étudiés correspondent aux ports ouverts par divers virus/vers/chevaux de Troie. Si votre politique de sécurité autorise le balayage des ports ouverts sur les postes de travail ou les serveurs, il peut s'avérer utile de le faire régulièrement afin de découvrir les machines potentiellement contaminées avant qu'un intrus ne le fasse à votre place.

L'analyse des journaux de votre pare-feu est une source pertinente d'informations pour la sécurité de votre réseau et de vos systèmes. Cela peut vous aider à anticiper des incidents en remarquant par exemple des activités anormales. Le CERTA peut vous aider dans ce travail d'analyse.

6.6 Réagir aux incidents de sécurité

Organisez-vous pour réagir aux incidents de sécurité, en particulier, pour assurer une certaine continuité dans les équipes d'administration et de sécurité.

Le CERTA a pour mission de vous aider à répondre aux incidents de sécurité informatique.

Ne traitez pas les dysfonctionnements des machines à la légère. Dans certains incidents dans lesquels le CERTA intervient, les administrateurs des machines font spontanément part de petits dysfonctionnements inexplicables et d'apparence anodine qui s'avèrent, au cours de l'analyse, être liés à un incident majeur de sécurité. N'hésitez pas à prendre contact avec le CERTA si vous constatez de l'activité sur les ports décrits ci-dessus.

6.7 Former et sensibiliser les utilisateurs

La sécurité d'un système d'information doit reposer sur une approche de défense en profondeur. Cela signifie, entre autres choses, que l'utilisateur est partie prenante de la sécurité. Sa vigilance, son niveau de formation et de sensibilisation participent à la sécurité du système. C'est pourquoi il est essentiel de prévoir des séances de formation et de sensibilisation des utilisateurs, acteurs de la sécurité. Pour vous aider dans ces actions, l'ANSSI dispose d'un centre de formation :

http://www.ssi.gouv.fr/site_rubrique67.html

7 Les bulletins d'actualité

L'objectif des *bulletins d'actualité* est de fournir une illustration par l'actualité récente de certaines mesures de sécurité pragmatiques à appliquer. Bien que par nature *a posteriori*, cette illustration a vocation à servir de base pour tirer des enseignements plus généraux à même de protéger contre des incidents futurs.

L'« actualité » est donnée par l'analyse de machines que le CERTA réalise dans le cadre de ses missions. Un fait est jugé d'actualité, s'il est à la fois récent et significatif, c'est à dire recoupé par différentes analyses.

Les *bulletins d'actualité* n'ont pas la prétention de constituer des statistiques fiables de l'activité informatique malveillante, mais ce qui nous semble avoir beaucoup plus d'intérêt, de montrer à partir d'exemples concrets, réels et anonymisés comment découvrir que l'on est ou a été attaqué et comment limiter l'impact de ces attaques.

La qualité des *bulletins d'actualité* sera améliorée grâce à votre participation. Si vous souhaitez participer, prenez contact avec le CERTA en accord avec votre chaîne fonctionnelle de la sécurité des systèmes d'information.

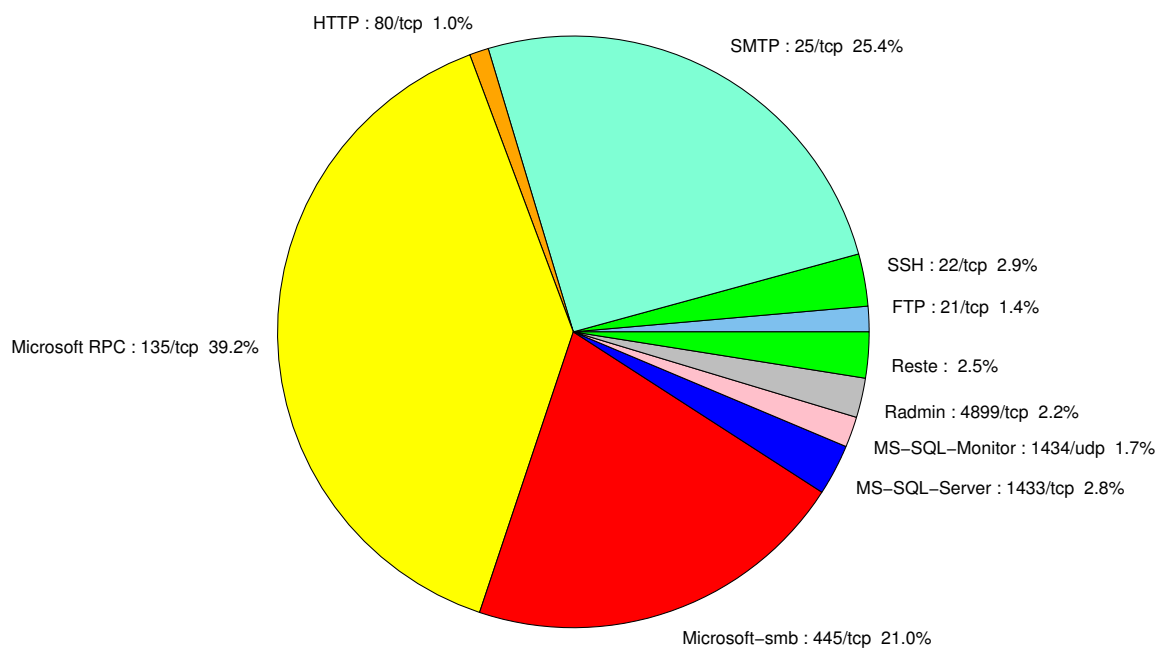


FIG. 1: Répartition relative des ports pour la semaine du 12 au 18 mars 2010

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	CERTA-2003-AVI-132 CERTA-2004-AVI-064 CERTA-2004-AVI-066 CERTA-2006-AVI-040
22	TCP	SSH	–	CERTA-2003-AVI-152 CERTA-2006-AVI-100
23	TCP	Telnet	–	CERTA-2003-AVI-209 CERTA-2003-AVI-131 CERTA-2007-ALE-005-001
25	TCP	SMTP	–	CERTA-2006-AVI-124 CERTA-2006-AVI-135
42	TCP	WINS	–	CERTA-2004-AVI-384
69	UDP	IBM Tivoli Provisioning Manager	–	CERTA-2007-AVI-320
80	TCP	HTTP	–	CERTA-2004-AVI-195 CERTA-2004-AVI-239 CERTA-2006-AVI-055 CERTA-2006-AVI-069 CERTA-2006-AVI-156 CERTA-2006-AVI-315
106	TCP	MailSite Email Server	–	– CERTA-2007-AVI-008
111	TCP	Sunrpc-portmapper	–	CERTA-2003-AVI-052
119	TCP	NNTP	–	CERTA-2004-AVI-340
135	TCP	Microsoft RPC	–	CERTA-2003-ALE-002 CERTA-2003-AVI-111 CERTA-2004-AVI-127
137	UDP	NetBios-ns	–	CERTA-2004-AVI-031
139	TCP	NetBios-ssn et samba	–	CERTA-2004-AVI-368 CERTA-2003-AVI-168 CERTA-2004-AVI-126 CERTA-2005-AVI-051 CERTA-2005-AVI-213 CERTA-2005-AVI-302 CERTA-2005-AVI-398 CERTA-2006-AVI-283 CERTA-2006-AVI-338 CERTA-2007-AVI-321
143	TCP	IMAP	–	CERTA-2005-AVI-185
389	TCP	LDAP	–	CERTA-2003-AVI-102 CERTA-2003-AVI-068 CERTA-2003-AVI-041 CERTA-2003-AVI-004 CERTA-2004-AVI-126 CERTA-2007-AVI-294
427	TCP	Novell Client	–	CERTA-2006-AVI-538
443	TCP	HTTPS	–	CERTA-2003-AVI-156 CERTA-2004-AVI-126 CERTA-2004-AVI-247 CERTA-2004-AVI-343 CERTA-2007-AVI-153
445	TCP	Microsoft-smb	–	CERTA-2004-AVI-053 CERTA-2003-AVI-105 CERTA-2004-AVI-126 CERTA-2005-AVI-051 CERTA-2005-AVI-302 CERTA-2006-AVI-283

				CERTA-2006-AVI-338 CERTA-2007-AVI-321 CERTA-2007-ALE-010
445	UDP	Microsoft-smb	–	CERTA-2007-ALE-010
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	CERTA-2006-AVI-232
1433	TCP	MS-SQL-Server	–	CERTA-2002-ALE-006
1434	UDP	MS-SQL-Monitor	–	CERTA-2002-AVI-157
2100	TCP	Oracle XDB FTP	–	CERTA-2005-ALE-002
2381	TCP	HP System Management	–	CERTA-2006-AVI-248
2512	TCP	Citrix MetaFrame	–	CERTA-2006-AVI-491
2513	TCP	Citrix MetaFrame	–	CERTA-2006-AVI-491
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	CERTA-2006-AVI-221
3104	TCP	CA Message Queuing	–	CERTA-2007-AVI-331
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	CERTA-2004-AVI-062 CERTA-2004-AVI-186 CERTA-2004-AVI-316 CERTA-2004-AVI-348
3268	TCP	Microsoft Active Directory	–	CERTA-2007-AVI-294
3306	TCP	MySQL	–	–
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	CERTA-2001-AVI-165 CERTA-2006-AVI-212 CERTA-2006-AVI-297
5151	UDP	IPSwitch WS_TP	–	CERTA-2007-AVI-312
5151	TCP	ESRI ArcSDE	–	CERTA-2007-AVI-367
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	CERTA-2006-AVI-198 CERTA-2006-AVI-299
6014	TCP	IBM Tivoli Monitoring	–	CERTA-2007-AVI-183
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	CERTA-2005-AVI-293
6101	TCP	Veritas Backup Exec	–	CERTA-2005-AVI-024
6106	TCP	Symantec Backup Exec	–	CERTA-2007-AVI-303
6129	TCP	Dameware Miniremote	–	CERTA-2003-AVI-214 CERTA-2005-AVI-326
6502	TCP	CA BrightStor ARCserve Backup	–	CERTA-2007-AVI-029
6503	TCP	CA BrightStor ARCserve Backup	–	CERTA-2007-AVI-029
6504	TCP	CA BrightStor ARCserve Backup	–	CERTA-2007-AVI-029
8080	TCP	IBM Tivoli Provisioning Manager	–	CERTA-2007-AVI-153
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	CERTA-2005-AVI-229 CERTA-2005-AVI-313
10080	TCP	Amanda	MyDoom	–
10110	TCP	IBM Tivoli Monitoring	–	CERTA-2007-AVI-183
10916	TCP	Ingres	–	CERTA-2007-AVI-275-001
10925	TCP	Ingres	–	CERTA-2007-AVI-275-001
12168	TCP	CA eTrust antivirus	–	CERTA-2007-AVI-217
13701	TCP	Veritas NetBackup	–	CERTA-2005-AVI-447
18264	TCP	CheckPoint interface	–	CERTA-2005-AVI-310
54345	TCP	HP Mercury	–	CERTA-2007-AVI-075
65535	UDP	LANDesk Management Suite	–	CERTA-2007-AVI-176

TAB. 2: Correctifs correspondant aux ports destination des paquets rejetés

port	pourcentage
135/tcp	39.17
25/tcp	25.4
445/tcp	21.01
1433/tcp	2.92
22/tcp	2.85
4899/tcp	2.36
1434/udp	1.67
21/tcp	1.39
80/tcp	1.18
2967/tcp	0.76
1080/tcp	0.69
3389/tcp	0.41
3128/tcp	0.34
3306/tcp	0.13
10080/tcp	0.06

TAB. 3: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Correctifs correspondant aux ports destination des paquets rejetés	7
3	Paquets rejetés	8

Gestion détaillée du document

19 mars 2010 version initiale.